Planning Considerations for Interfacing Emergency Communications Centers with FirstNet

SEPTEMBER 2019

MICHIGAN'S PUBLIC SAFETY BROADBAND PROGRAM
GEORGE W. ROMNEY BUILDING ● 111 SOUTH CAPITOL AVENUE ● LANSING, MICHIGAN 48933
www.michigan.gov/MIPSB ● 517-335-3727

Table of Contents

1 Introduction

Under the State and Local Implementation Grant Program 2.0 (SLIGP 2.0), the Michigan Department of Technology, Management and Budget (DTMB) assessed the readiness of emergency communication centers (ECCs) in the state for implementation of the First Responder Network Authority (FirstNet)'s nationwide public safety broadband network (NPSBN). A representative sample of urban, suburban, and rural ECCs were visited and surveyed. The purpose was to gain an understanding of the challenges faced in implementing Next Generation 911 (NG911) and other technologies and the integration of such systems with the NPSBN. Another goal was to measure the level of interest in the NPSBN and to identify proposed uses of the network as it is deployed throughout Michigan.

ECC administrators were asked to share their concerns and perceived challenges of integrating the NPSBN into their operations. This planning document addresses those challenges along with others that have been identified as critical to the integration of the NPSBN with ECC operations.

The NPSBN deployment is expected to eliminate many constraints concerning the ability of field responders and ECCs to share critical data with each other. Implementation and adoption of the NPSBN and NG911 systems will enable ECCs to access additional data, video, and images from citizens and field responders, thereby providing a tool that vastly improves situational awareness. This, in turn, will enhance field responder safety and their ability to protect citizens and property, improving emergency response. Convergence of the NPSBN and NG911 is expected to remove most of the constraints regarding the reception and retransmission of data, text, video, and images.

Multimedia data submitted by persons reporting emergencies and then made available to field responders has the potential to improve the efficacy of emergency responses. This will be accomplished in myriad ways. First responders—police, fire/rescue, emergency medical services (EMS) and 911 telecommunicators (call-takers and dispatchers)—will be informed of conditions at the scene of an emergency. Information regarding an incident from field responders will be shared with other responders, medical facilities and, in some cases, the public. In particular, availability of real-time video from field responders creates an opportunity to improve the safety of both the responders and the public by improving situational awareness, by having remote "eyes" on incidents as they unfold.

This planning document[1] is intended to familiarize those who are responsible for ECC operations with the technology and operational challenges that can be anticipated when FirstNet's NPSBN and NG911 systems converge. Deployment of the NPSBN and NG911 systems make available the network technology, capacity, and capability that will permit the sharing of multimedia data (images, video, and other digital data) between the public, ECCs, and field responders.

[1] Funding for this project was provided by the State and Local Implementation Grant Program (SLIGP) of the National Telecommunications and Information Administration (NTIA) as established by Title VI of the Middle Class Tax Relief and Job Creation Act of 2012, Public Law 112-96.

To realize the vision of a converged public safety communications system, material changes will be required regarding the technology, systems, processes, policies, and personnel training that exist in ECCs. It is the intent of this planning document to outline the steps that may need to be completed to implement a functional, converged system taking into consideration these key elements:

- Technical
  - Policy requirements
  - Infrastructure implications
  - Cybersecurity risks
  - Data storage
  - Data analytics
  - Interface development
  - Standards adoption by vendors
- Operations
  - Policy and procedures
  - Workflows
  - Data analysis
  - Workforce implications
  - Training needs
- Governance
  - Regulatory and legislative constraints
  - Facilities structural implications
- Staff Support
  - Personnel development
- Financial
  - Funding

Multimedia data streams made possible by the NPSBN and NG911 convergence have the potential to provide ECCs with unprecedented situational awareness information that will make both telecommunicators and field responders more effective and thus improve emergency response. However, to leverage this capability fully, ECC managers will be confronted with technical, financial, operational and personnel-development challenges. As with implementation of other transformational technologies, there will be cultural and procedural changes as well that will need to be anticipated and managed.

This document is neither a needs assessment nor a design for a specific ECC. Rather, it describes how a converged system can operate and considerations leading to detailed planning and design.

1.1 Acknowledgments

DTMB extends its appreciation to the staff of the public safety agencies, public safety answering points (PSAP), and emergency operations centers (EOC) that completed surveys and to the following ECCs for sharing their experience and insight during site visits:

- Eaton County Central Dispatch / Emergency Operations Center
- Kent County Sheriff's Office Dispatch Operations
- Marquette County Central Dispatch / Emergency Operations Center
- Michigan State Police Regional Communications Centers
- Michigan State Police Intelligence Operations Center
- State of Michigan Emergency Operations Center

1.2 Planning Guide Objective

The objective of the SLIGP 2.0 – ECC Integration Planning Project was to understand the impacts and challenges facing ECCs concerning the implementation of FirstNet's NPSBN and to determine the level of interest in integrating emerging technologies (such as NG911), as well as dispatch systems and other operational technologies, with FirstNet's NPSBN. This document provides guidance based on the results of the surveys, and interviews and observation of the selected ECCs. It also provides analysis of the steps that reasonably can be expected for provisioning basic services—such as improved voice communications interoperability and wireless data access to existing applications—and for implementing advanced services, such as real-time video, to and from first responders. In cooperation with ECC representatives, lessons-learned will be identified and model policy and guidance will be developed for integration of NG911 and FirstNet's NPSBN.

1.3 Existing Technology Overview

A PSAP, which comprises a subset of an ECC, makes the connection between persons reporting emergencies and the field responders who provide emergency services to the public. Emergencies may be reported by the public to the PSAP through the universal emergency telephone number 911 or by field responders using other communications systems.

Public calls to 911 are initiated from persons using traditional wireline telephones, wireless devices, and Voice over IP (VoIP) telephony. More than 75 percent of 911 calls are made from wireless devices. Traditional wireline telephones are used for about 15 percent of 911 calls and VoIP for less than 10 percent.

Technology used to route 911 calls is based upon archaic wireline telephony standards and equipment. An evolution was required to accommodate wireless 911 calls and to provide location data. Neither the routing nor the location data provided by existing wireless 911 systems are accurate to a level that provides consistently accurate results. These network weaknesses have led to the development of an NG911 standard that is slowly being implemented. Known as the third iteration of the National Emergency Number Association (NENA) Functional and Interface Standards for NG911 (NENA i3), the solution supports end-to-end Internet Protocol (IP) connectivity.[2]

[2] Functional & Interface Standards for NG9-1-1 (i3)

Communications between the PSAP and field responders since the 1930s has been conducted on land mobile radio (LMR) systems, aka two-way radio. LMR systems are traditionally push-to-talk (PTT) systems that provide dedicated radio channels or talkgroups that are shared by public safety operational groups organized by function and/or location. Most public safety operations are coordinated through voice communications. Some computer-aided dispatch (CAD) and incident information, largely text-oriented, is provided to mobile computers through a private mobile data system or through a wireless carrier ("cellular") network. The figure below depicts the current emergency communications ecosystem.

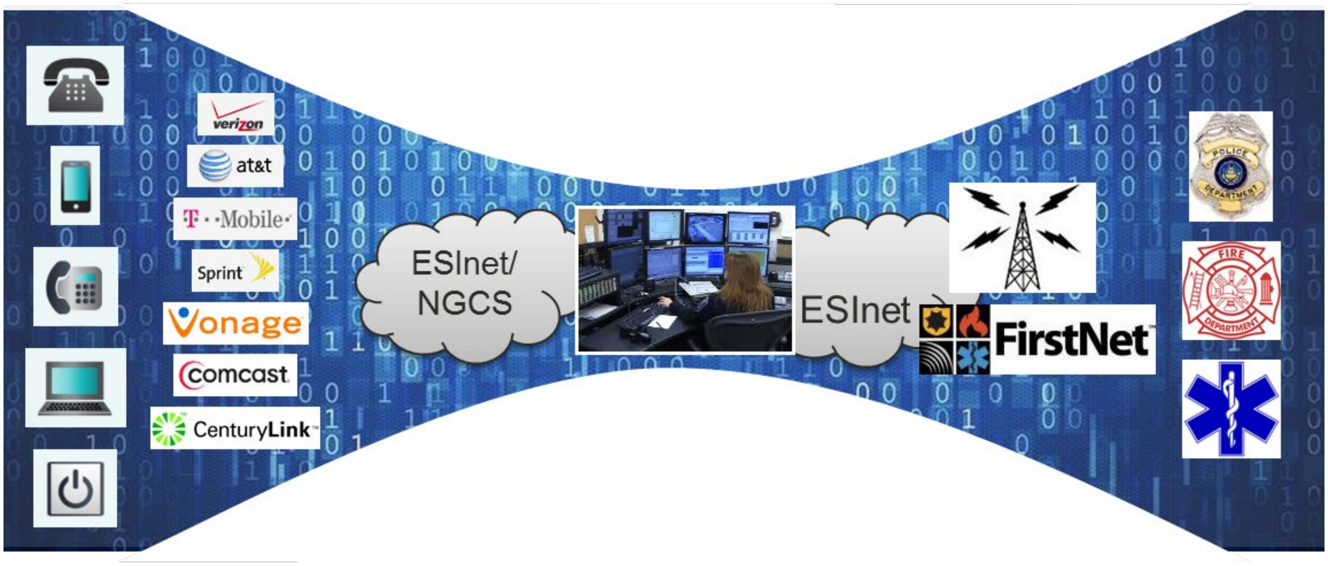

Figure 1: Current Emergency Communications Ecosystem

1.4 Future Technology Environment

NG911 systems and FirstNet's NPSBN will form a standards-based, broadband, end-to-end public safety communications platform to enable the connection between the public, the PSAP, and field responders. This platform will create a tremendous opportunity to greatly enhance public safety response and improve outcomes. Field responders will have timely access to mission-critical data that support the performance of their jobs. Mission-critical data includes both databases that store critical information as well as real-time data that improves situational awareness.

PSAPs will serve in a unique role as the convergence point between the two technologies and networks and will facilitate data sharing, providing another level of situational awareness for the field responders.

- NG911 provides the PSAP with improved location data from wireless 911 callers.
- IP-based broadband networks are being deployed for emergency communications in conjunction with NG911.

- Emergency Services IP Networks (ESInets) are IP networks that provide connections between originating telecommunications networks and PSAPs to enable improved call routing and transfer, data sharing, and increased backup/resiliency options between PSAPs.
- ESInets provide the infrastructure upon which Next Generation Core Services (NGCS) operate. Among other functions, NGCS enable 911 callers to confidently share video, images, text and other data with ECCs. Broadband networks such as FirstNet's NPSBN provide the capability to share this data securely between the ECCs and field responders.
- An additional but non-native component of NG911 is the additional data repository (ADR). The information available in the ADR could be shared with field responders via a broadband network such as the NPSBN.
- Modern public safety radio systems have enhanced network services that support data and Global Positioning System (GPS) location services.

FirstNet and its contractor AT&T are deploying the NPSBN, which is an IP-based, nationwide wireless broadband network that will accommodate transport of mission-critical data in the near term, with an expected ability to support mission-critical, push-to-talk voice communications sometime in the future. The figure below depicts this future emergency communications ecosystem.

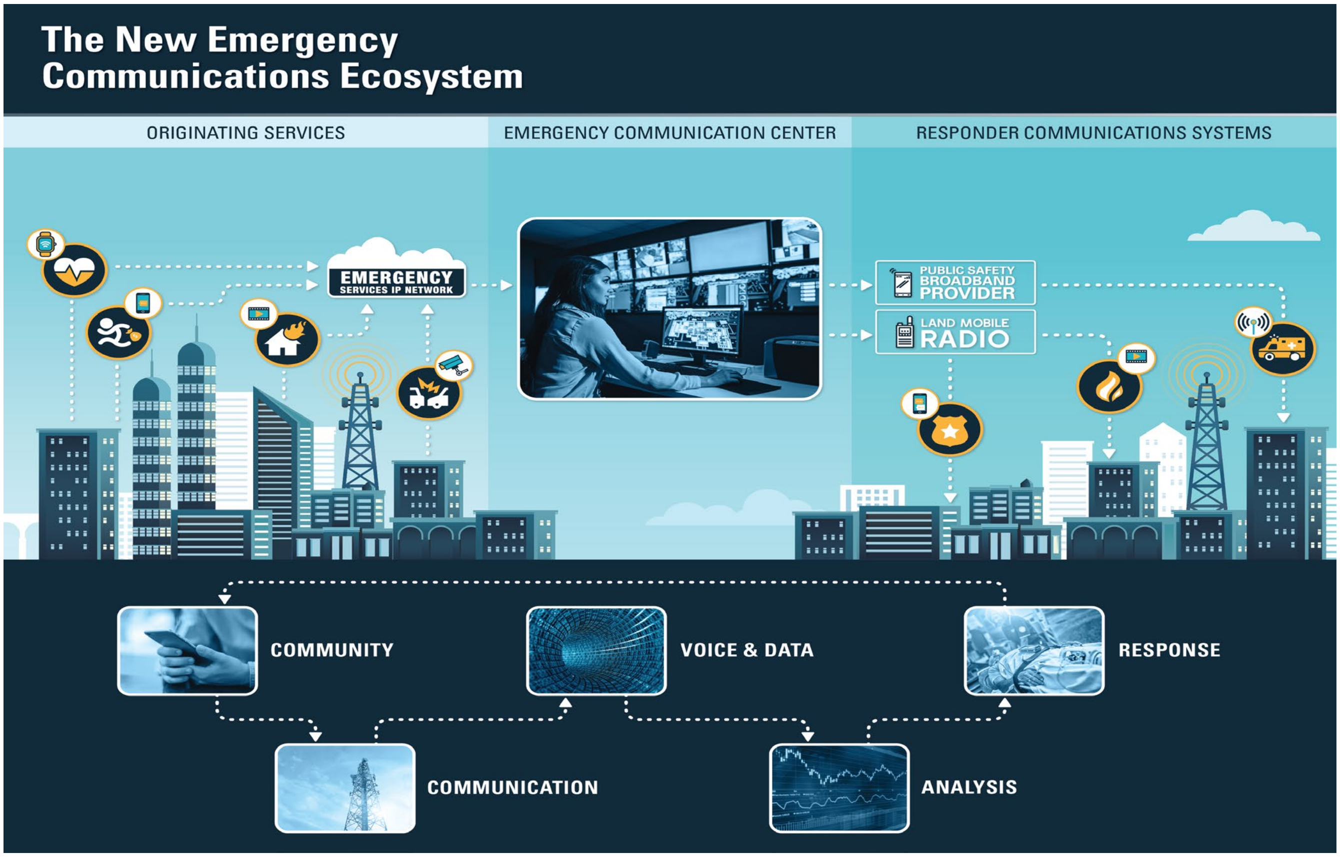
The New Emergency Communications Ecosystem
ORIGINATING SERVICES
EMERGENCY COMMUNICATION CENTER
RESPONDER COMMUNICATIONS SYSTEMS
EMERGENCY SERVICES IP NETWORK
PUBLIC SAFETY BROADBAND PROVIDER
LAND MOBILE RADIO
COMMUNITY
VOICE & DATA
RESPONSE
COMMUNICATION
ANALYSIS

Figure 2: Future Emergency Communications Ecosystem

2 Common Integration Planning Considerations

The modern public safety communications ecosystem is a technologically sophisticated environment that is essential to effective emergency response operations. The more complex the ecosystem gets and the faster it expands, the more difficult it is to maintain an understanding of the relationships that will be impacted and the downstream implications of implementing new or cutting-edge technology. Regardless of the solution being contemplated, several considerations exist that are common across the board.

Future public safety communications systems will be IP-based and as such will enable data sharing between agencies that provide improved location information and situational awareness from previously inaccessible data. Increased access to and analysis of data has the potential to enhance emergency response and help keep field responders safer. However, data sharing will require memoranda of understanding (MOU) that outline the types and uses of data to be shared between participating public safety and public service agencies, including ECCs. Examples of such data include the following:

- Multimedia data from persons reporting emergencies
  - Videos or digital images of the scene
- Multimedia data originating from field responders
- Multimedia data from video surveillance and/or traffic camera networks
- Schools' panic alarm and video systems

At the ECC there is a requirement for technology enhancements, policy development, and training to realize the potential lifesaving value of this data. This document will examine many of the key areas that should be considered during planning.

2.1 Information and Change-Management Framework

To answer the numerous questions that agencies have regarding operationalizing integration of their ECC functionality with FirstNet's NPSBN and other emerging technologies (e.g., NG911) we need to discuss the importance of an information and change-management framework.

An information and change-management framework is critical for supporting effective decision-making and determining whether to implement any of the solutions that follow. An information and change-management framework provides the opportunity to critically explore the pros, cons, and requirements of any new implementations. An information and change-management framework to address transformational change should include analysis of the following considerations every time a solution is presented to an organization:

- Technology policy requirements
- Technology infrastructure constraints
- Workforce implications (both inter- and intra-agency)
- Operational workflows, policies, and procedures

- Training needs
- Governance policies
- Regulatory and legislative constraints
- Funding
- Facilities structural constraints
- Metrics for measuring success

The outcomes of the change-management workflow should generate positive responses to at least one, or more, of the four questions, identified below before an executive sponsor signs the project charter and gives approval to moving forward. These responses should indicate that the proposed solution is expected to improve emergency response.

Does the proposed implementation:

- Improve situational awareness?
- Improve decision-making capabilities?
- Decrease response times?
- Have the potential to save lives?

If those vendors proposing an implementation cannot articulate how their solution will answer these questions and how the interface works, it may be in the best interest of the organization to say no to the solution at this time. If the organization cannot articulate how it sees the solution answering these questions, it also may be in the best interest to hold off on the solution until those questions can be answered.

For those implementations that are completed, it is essential to have predetermined metrics to ensure that the solution is providing the functionality and outcomes that were anticipated. If the metrics are not being realized, the change-management team will need to work with the vendor to determine whether anything can be done to improve the solution's functionality, or whether the solution or service should be removed. Keeping ineffective technologies and/or services in play is wasteful and can have a negative impact on emergency response services.

A best practice would be to compile the outcomes of this analysis in a document that identifies the following:

- Project scope
- Objectives and risks
- Organization and staffing
- Decision-making structure and approach
- Initial resource requirements

This document essentially is an executive summary that also can serve as a business case for the suggested solution. Once compiled, the information and change-management review team, along with the

executive sponsor, would review the document and make an educated go/no-go decision. This is an opportunity—before anything is inked and time and money are committed—for stakeholders to evaluate the solution's feasibility and value for improving emergency response outcomes.
It also is important to plan for the transition from solution implementation to managing its lifecycle. This planning should include a policy for capturing several attributes for each solution. These attributes should be gathered, compiled and kept on file—preferably in a database—to manage the solution's lifecycle and to promote disaster recovery efforts should they be needed.

2.1.1 Basic Service Integration

Once a decision has been made to implement a specific solution, there are two integration steps that should be contemplated during planning: basic and advanced.

Basic service integration is the incremental improvement of legacy ECC functionality by the introduction of the NPSBN. The first step involves basic service integration between ECCs and the NPSBN. This step involves wireless data services, interoperability with existing LMR voice systems, and interoperability of PTT functionality with other public safety entities on a Long-Term Evolution (LTE) network. Planning for basic service integration involves the following action steps:

2.1.1.1 Action Steps

- Create a planning document, outlining the specific steps, timeline, and task deliverables.
- Identify the technical, operational, and policy needs of ECCs and field responders pertaining to ECC and NPSBN integration, using a mix of interviews, assessments, and a needs analysis.
- Develop a model of the integration steps, policies, and costs.

2.1.2 Advanced Service Integration

The second step towards transformation of ECC technology, which involves exploitation of the NPSBN's broadband capabilities, is advanced service integration. This step is focused on collecting multimedia data from multiple sources and then sharing the data between the ECC and field responders. This segment of the project is focused on the definition of the technologies and processes required to enable the capture, analysis, distribution, display, and archival of text, images, and video content between the 911 caller, 911 call-handling equipment (CHE), and CAD systems at the ECC, and with wireless devices used by field responders that operate on the NPSBN.

When advanced service integration is completed, examples of multimedia data that could be shared include:

- Multimedia data from 911 callers, such as video or digital images
- Field-originated videos, such as from responder body-worn or dashboard cameras
- Location data of callers and field responders
- Video from public or private closed-circuit television (CCTV) or surveillance cameras

- Data received from sensors or other automated systems

2.1.2.1 Action Steps

- Create a planning document, outlining the specific steps, timeline, and task deliverables.
- Develop a user-level description of the integration of the NSPN with NG911 and ECC systems under various operational scenarios.
- Gather requirements from the 911 and field responder communities to identify the stakeholders' specific needs for integrating these systems.
- Based on stakeholder input, determine the technical, operational, policy, and staffing requirements to implement the advanced service integration.

2.2 Requirement for a Secure Connection to the NG911 ESInet

Cybersecurity planning and execution should be driven from ECC leadership through the organization, not managed as just another information technology (IT) project. It should be understood that managing an appropriate cybersecurity strategy and plan will be an ongoing journey and not a one-time event. Any network, such as an ESInet or the NPSBN, that facilitates the transport of a public safety application, and all other networks that are physically connected to such networks, should be considered to be within scope.

Leveraging established and appropriate IT standards provide a clear direction for near-term and ongoing cybersecurity planning and execution. For instance, the Task Force for Optimal PSAP Architecture (TFOPA) published *Working Group 2: Phase II Supplemental Report: NG9-1-1 Readiness Scorecard*, in December 2016.[3] It identified cybersecurity as a key component of the NG911 self-evaluation process.

2.3 Effect of Michigan Legislation

2.3.1 Emergency 911 Service Enabling Act (Act 32 of 1986)

The FirstNet NPSBN enables agencies to leverage the capabilities created through the numerous applications never before accessible. These new capabilities make legislation, such as Chapter 484 of the Michigan Compiled Laws, relevant to this new ecosystem. Chapter 484 of the Michigan Compiled Laws established the 911 emergency telephone system for the state. Section 484.1207 regulates automated connections to the 911 system and states "The installation of automatic intrusion alarms and other automatic alerting devices which cause the number 9-1-1 to be dialed shall be prohibited in a 9-1-1 system."

A plain reading of this law indicates that alternative means of delivering an alarm to an ECC other than by connection to a telephone company network and dialing 911 are prohibited. However, in an NG911 environment and with the ability to enable numerous applications through the FirstNet NPSBN, numerous

[3] https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG2_Supplemental_Report-120216.pdf

automated devices will be capable of transmitting data to an ECC, either to report an emergency or to provide relevant information regarding a reported or unreported emergency. As it is reported to the ECC, field responders will have access to the information through the NPSBN.

It is apparent that a regulatory framework may be required to manage the anticipated increase in data arriving at an ECC through network connections other than those provided by the 911 network. Data-formatting standards will be needed to ensure that the data sent by persons or things that are reporting emergencies can be received, viewed, stored, routed, and searched using open standards-based ECC software.

While restricting competition and innovation in methods of reporting emergencies is not desirable, neither is a proliferation of untested, non-standard, or insecure applications and devices. Devices that heretofore have not been considered as sources of emergency calls will appear in the marketplace. Of particular concern are Internet of Things (IoT) devices, which already number in the billions. IoT devices already have been identified as vulnerable to hacking and exploitation in botnets configured for distributed denial of service (DDOS) attacks. With billions of devices attached to the internet it will be necessary to regulate what information, if any, they can be programmed to report to a PSAP. Many states and localities prohibit automatic-dialer alarm systems from dialing 911. In most cases, ordinances or laws do not contemplate reporting of emergencies via the internet. Amendments to such laws and ordinances likely will be required.

Like automatic-dialer alarm systems, it is likely that IoT devices that are reporting alarm conditions will need to be routed to an alarm-monitoring center for screening. For example, IoT devices may be programmed to report a power outage. Often in wind storms, there will be power surges and brief outages that have the potential to trigger thousands of alarms. While this information may be useful for a utility company or facilities manager, the potential volume of calls could overwhelm an ECC. If screened, or processed by a data-analytics application, the information could be reduced to a concise data visualization, such as a map, that would be useful to ECC staff.

3 Targeted Planning Guidelines

Public safety communications have reached an inflection point. Previous voice-centric communications are being replaced or supplemented by data-centric technology. This evolution is affected by the following:

- Wireline-to-Wireless Transition – Access to data provided by numerous applications—such as a heart rate measured by a smartwatch or fitness monitor—will be enabled to allow the ECC to capture and forward that information to field responders through the NPSBN. More smartphone applications related to biomedical monitoring are being developed and introduced as more sophisticated wireless devices enter the marketplace every day. Today there are more wireless subscriptions in the United States than the population. More than 300 million smartphones are being used in North America and at least 80 percent of 911 calls now originate from wireless devices. The National Health Interview Survey of 2017 indicated that in some states as many as 62 percent of households only use wireless phones and do not have wireline telephone service. The legacy 911 network was based on circuit-switched telephony that is being replaced by IP-based networks. The transition to IP-based 911 networks nationwide will require significant changes in ECC equipment and operations to take advantage of the additional data made available, which can be shared with field responders via the NPSBN.

- Emergence of Location-Based Data – The availability of location-based data from wireless devices allows suitably equipped field responders to be located whether inside or outside their vehicles. This is done through use of applications connected to the ECC or other field responders through the NPSBN. This capability has the potential to improve field responder safety and effectiveness when in foot pursuits, when establishing perimeters at a crime scene, or when coordinating searches. Nearly all wireless devices contain a GPS transceiver that provides accurate location data. This data often is more precise and dynamic than the location provided by network-based, location-determination technology that depends on triangulation or time-difference-of-arrival (TDOA) techniques. Commercial wireless applications have widely adopted location-based data for everything from determining the lowest nearby gasoline price to improving pizza delivery to ride sharing. ECC use of such data to determine the location of 911 callers lags the commercial applications. Newer-generation smartphones using enhanced services from Android, known as Emergency Location Service (ELS), or Apple's Enhanced Emergency Data Service, provide enhanced caller location information to the ECC. Location data is sent via Short Message Service (SMS) or Hypertext Transfer Protocol, Secure (HTTPS), which are open, operating system (OS)-agnostic telecommunications carrier protocols.

- Traditional LMR networks – The existence of the FirstNet network creates the opportunity for LMR-to-NPSBN PTT interoperability and the need to plan for interfaces to the ECC. LMR is voice centric and operates on narrowband radio channels. Such channels do not provide data-throughput rates that are adequate to support more than short texts, data bursts, or status messages. Most LMR systems are owned by state and local governments. Historically, the Federal Communications Commission (FCC) has failed to provide enough radio spectrum to support the nation's public safety entities in a common frequency band. The use of disparate frequency bands and technologies has been—and continues to be—an impediment to interoperability. Moreover, the size of the public safety equipment market is very small compared with the market for commercial wireless networks. Consequently, LMR equipment costs are high compared with smartphones, innovation is limited because economies of scale are lacking, and radio spectrum incompatibility requires expensive workarounds to achieve interoperability. It is not suggested that the NPSBN at its present state of deployment is suitable for a total replacement of LMR. Interoperability between the two technologies can be provided through PTT interfaces. Planning for such interoperability can result in the provision of enhanced capabilities such as operational support of responses to large-scale events outside the normal area of operation, support of covert operations, and interservice communications between other classes of primary and extended primary users.

3.1 Planning for Access to Primary ECC Systems through FirstNet

Planning for the integration of primary ECC systems with the NPSBN to provide new or improved access from mobile devices is an important first step in improving the effectiveness of first responders through enhanced access to data. Mobile computers and smartphone-based devices can provide browser access to many primary ECC systems making them simpler and more intuitive to use.

3.1.1 Call-Taker Interfaces

A typical call-taker position in an ECC will continue to be equipped with a CAD system computer with one or more screens for the following: call entry, display of calls pending dispatch, and a mapping/geographic information system (GIS) interface to display the status of field responders. 911 CHE (previously referred to as customer premises equipment, or CPE) will have a separate display or two. As additional sources such as video are introduced into the ECC, additional computers and screens will be needed until systems can be integrated fully.

3.1.2 Computer-Aided Dispatch Interfaces

Multimedia data servers require an interface with the ECC's CAD system. A standard data interface will be necessary to promote widespread adoption of the capability and to reduce implementation costs.

The purpose of the interface is to associate the calls-for-service records with any accompanying multimedia data. It should provide a simple, "one-key" transfer function to transmit multimedia data via the NPSBN to personnel equipped with mobile or portable computers and/or smartphone-based devices.

An incident number should be shared between the CAD system and the multimedia data server for archival and retrieval purposes. This incident number should be searchable via suitably equipped wireless devices as well as authorized agency computer network users.

A geofenced search function integrated with the CAD system would be useful to locate any multimedia data from prior events reported at or near an address.

Most CAD systems today are not configured to receive the text, video, and image data that can be sent by callers to an NG911 system and then distribute that data to field responders. Even when such data can be received by an ECC, it often cannot be forwarded to field responders in a timely manner, or even at all. Legacy CAD systems may have an interface with an existing wireless broadband network for mobile applications. Such interfaces may have been implemented in conjunction with a 3G wireless network such as 1xRTT.[4] In other cases, a mobile data interface may not have been provided. Functions that need to be addressed via interfaces between the CAD system and FirstNet's NPSBN are as follows.

3.1.3 Records Management System Interfaces

An interface between the multimedia data system and the records management systems (RMS) used by EMS, fire and law enforcement agencies is a desirable function. Cross referencing of multimedia data and incident reports is an important function for training, evidence management, management of public complaints, litigation and other purposes within the public safety agencies.

[4] Single-carrier radio-transmission technology.

3.1.4 Interfaces Between Call-Takers and Radio Dispatchers

Still images or short video clips that are received by 911 call-takers from a person reporting an emergency should be attached to an incident dispatch record when transferred to a radio dispatcher. This information also should be accessible from a field responder equipped with a mobile computer or smartphone. Generally, this can be accomplished by an interface to the CAD system via FirstNet's NPSBN.

3.2 Sources of Multimedia Data Coming into the ECC

The following are guidelines and considerations that are specific to various technology categories that, if properly interfaced with the ECC, may provide enhanced information to emergency responders via the NPSBN.

3.2.1 Alarm Processing

The Automated Secure Alarm Protocol (ASAP) was developed jointly by the Association of Public-Safety Communications Officials (APCO), the Central Station Alarm Association (CSAA), and the National Law Enforcement Telecommunications System (NLETS). The program—an early example of an interface known as ASAP to PSAP—has been in place since 2011. The program enables the transfer of alarms from a central-station alarm-monitoring facility into a participating PSAP's CAD system via NLETS. Alarms that have been screened by the central-station alarm company before transmission do not dial 911 but make use of the NLETS message switch. Fifty PSAPs are participating in the program and another 12 are testing or implementing this ability. Meanwhile, 23 alarm-monitoring companies participate in the program and another 11 are in test or implementation phases.

Stated advantages of ASAP are:

- Reduced call-taker time spent entering alarm-generated information into the CAD system
- Improved information accuracy because there is no manual data entry
- Time needed to process alarms is reduced

3.2.2 Autonomous Vehicles

Information transmitted to the ECC will be available to field responders via the NPSBN, providing additional information that can be used to more efficiently respond to the emergency. Exactly how the data will be used is uncertain, but the development and road testing of autonomous vehicles are underway, which already has led to driverless vehicles in limited instances. Such vehicles will be equipped with light detection and ranging (LIDAR) and other sensors that will assist in collision avoidance. Autonomous vehicles also will be equipped with location-determination devices that will provide routing to a destination. Systems based on standards such as Cellular Vehicle to Everything (CV2X) will communicate information to other vehicles about speed and direction to avoid collisions. Autonomous vehicles may create new public safety challenges and will generate additional workload for ECCs. Autonomous vehicles will not always have a driver in the traditional sense. Therefore, there will not be a responsible person to handle, for example, a call for road service when the vehicle stalls, to provide registration and insurance information to a police officer, or to provide instructions on where a vehicle should be towed.

Autonomous vehicles will be equipped with wireless communications to provide notification of an emergency to a call center, such as OnStar,[5] or directly to an ECC.

Policies or laws will be needed to determine whether such automatic reports from autonomous vehicles will be routed through an NG911 system or through a private clearinghouse, such as RapidSOS's NG911 Clearinghouse. If calls are permitted to be routed to an ECC, the policies or law(s) will need to identify the type of acceptable calls—such as collisions, medical emergencies, fires, or panic alarms—from vehicle occupants.

3.2.3 Gunshot Detection Systems

Gunshot detection systems consist of acoustic sensors located in numerous locations where statistically gunfire is likely. The systems use forms of audio TDOA to provide a location for shots detected by the sensors. This data may be received by a service provider monitoring center that analyzes the data, determines whether the sound captured is a gunshot(s) and forwards that information to field responders. Analysis of the sounds can, in some cases, identify the type of weapon(s) from which the shots emanated. Various implementation permutations regarding this technology have occurred, including interface to the CAD system at an ECC. Location data can be sent to smartphones and mobile computers, depending on the interface chosen. The NPSBN can provide transport of this information to wireless devices affiliated with the network.

3.2.4 Enhanced Data Repositories

Smartphones and other connected devices can provide additional information about an incident that is valuable to ECCs. This data can include more precise call location as well as supplemental information about the caller, the calling device and the incident location. Sample media types today predominantly include user-entered caller information such as demographic data, emergency contacts or medical information. Additional information from 911 calls can be supported by applications such as RapidSOS's NG911 Clearinghouse, Carbyne's NG911 call-handling platform, and Smart911, which provides preloaded 911 caller profiles to the ECC.

Information provided by such applications includes the following:

- Enhanced caller information—name, address, phone number, image, medical information and more
- Additional data regarding the caller's location (e.g., Android's ELS)—supplemental 911 location data not provided by traditional carrier methods and based on smartphone technology.

[5] Any references in this document pertaining to current market offerings are included as exemplars of the current market and are not an endorsement of any particular product or vendor

The data processed and made available by ADRs is owned and managed by a plethora of independent databases typically available via connections to the public internet. As such, connections to these applications pose a risk to an agency's public safety communications system and must be protected with robust cybersecurity protocols, firewall protection or integration with a CHE platform.

3.2.5 Field Responder Safety Devices

Potential exists to enhance emergency response and improve citizen and field responder safety by communicating urgent data through the NPSBN to an ECC, a multimedia analysis unit, and/or the emergency responders. Urgent data that may be communicated includes biometric data about the physical wellbeing of an individual caller or field responder.

3.2.5.1 Field Responder Sensors

It is anticipated that field responders will use ruggedized smartphones, or devices that are based on smartphone technology, to interface with external sensor devices. Functions that will be provided by those sensors will include the capability of providing location and biometric information and transmit—manually or automatically—an emergency signal that triggers the transmission of that data. These devices need user interfaces appropriate for the type of application and a wireless method of connecting multiple external sensors. Development of such devices will be stimulated by the increase in users of the NPSBN. This functionality requires interfaces from the NPSBN to mapping systems used in the ECC and/or biometric-monitoring consoles at the incident command post or fixed location, such as an intelligence center.

A personal area network (PAN), also known as a body area network (BAN),[6] is a wireless network of wearable computing devices. BAN devices may be embedded inside the body (i.e., implants), may be surface-mounted on the body in a fixed position (i.e., wearable technology), or may be devices that are carried in clothes pockets, backpacks or other types of bags. Personal sensors—such as smartwatches, smart vests, and biometric vests equipped with physiological sensors that detect the user's body temperature, heart rate, and respiration rate—could relay vital real-time information on personnel to incident commanders, hospitals or the ECC. For example, a firefighter who—based on his/her biometric data—is about to suffer a cardiac event, could be taken off the line by an incident commander before tragedy strikes. For this to occur, connectivity between FirstNet's NPSBN and the wireless devices used by field responders, incident commanders, the ECC and/or multimedia analysis unit is required.

Indicators that a field responder is in a dangerous situation, location of a responder who is outside of a vehicle, and situational awareness provided by person- or dashboard-mounted cameras all are invaluable to the incident commander and ECC. Some devices may employ an emergency button, aka man-down button, to send a mayday signal and associated transmission of the user's location. An interface with the ECC's system(s) is needed to display unit identification and location information.

[6] https://www.dhs.gov/publication/personal-area-network-fact-sheet

The following identifies some of the data scenarios being contemplated:

- Holster sensors
  - Automatic initiation of an alert signal to the ECC and other field responders that a lethal or non-lethal weapon has been removed from its holster
  - Alert signal initiates transmission of location data

- Smartvest applications
  - Smart body armor has entered the marketplace that can initiate communications with an ECC, intelligence center, or other field responders when an impact consistent with a bullet, shrapnel or a knife strikes the vest. The vests use some form of wireless technology, typically Bluetooth, to communicate with a smartphone or LMR portable to automatically report the incident. Interface to the NPSBN typically will be through a smartphone-based LTE wireless device.

- Out-of-Vehicle Locations
  - Out-of-vehicle personnel, foot pursuits, searches, wildfire response, “bread-crumbing” functionality.
  - Accurate location data inside buildings is a challenge that has not been fully solved. Provision of in-building location was a requirement specified by FirstNet in its request for proposals (RFP).
    - The need to locate field responders inside buildings is complicated by the fact that GPS coverage inside of buildings is unreliable. The so-called “Z-axis” position is the subject of research and testing to enable identification (ID) of the responder’s vertical location, i.e., the building floor. This capability is also planned to provide the location of wireless 911 callers.
    - Development of next-generation Wi-Fi operating in millimeter-wave spectrum is underway; while current Wi-Fi networks are unable to provide location data, this capability is intended as an intrinsic function of the future iteration.
  - Body-worn equipment and sensors may use FirstNet’s NPSBN for connectivity to incident commanders, other field responders in the vicinity, an ECC and/or a situational awareness center (SAC). Display of the field responders’ location inside a building will require an application that interfaces with digital floor plan drawings and a low latency interface to the NPSBN. For this function, some considerations include:
    - Detailed floor plan data will need to be collected from fire-prevention inspections and building-permit applications.
    - Both plan and profile views at scale will be required.
    - Floor plans will need to be generated in a standard format that is readable and which can be displayed on a personal computer with a suitable application.
    - Georeferencing of the building plans will be required to provide a display of the location inside the building.
    - Floor plans must be downloadable with minimal latency to be usable by incident commanders and at the ECC and/or SAC.

An interface with the ECC’s CAD system will be required for archival and incident reference purposes.

3.2.5.2 Public Personal Sensors

Sophisticated physiological sensors have been developed that permit the detection of medical conditions such as an impending seizure, tachycardia, and abnormal blood sugar levels. These sensors may be interfaced to smartphones, smartwatches, or fixed network devices, such as Wi-Fi, that may be capable of sending text or multimedia data messages to others. Emergency responders receiving this information through the NPSBN will be able to communicate with the caller and the local hospital to determine whether the situation requires an emergency room or urgent-care clinic visit, which could lower the cost of the response to the caller and to the insurance company.

ECCs can anticipate receiving emergency calls from the public who may be equipped with smartphones or other electronic devices capable of using a wireless network to report an emergency. Because nearly every state, including Michigan, prohibits automatic dialing devices from dialing 911, calls from these devices may be delivered to a private alarm-monitoring facility that would relay call information to an ECC. Wireless devices operating on 4G and 5G networks will be capable of providing location data.
Most current- and prior-generation medical alert devices of the “I’ve fallen and can’t get up” type do not contain location-determining technology. Most such devices use the location of a wireline telephone subscriber’s address to provide private call centers with the location of the person. Several companies are now offering systems with a cellular GPS option.

Currently, the paradigm for medical alert sensors to notify emergency responders is through private call centers that accept and verify calls, then notify an ECC via a ten-digit telephone number. Limitations of the legacy 911 network constrain the transfer of emergency calls from a private call center to an ECC in a distant location. State laws often prohibit automatic-dialing electronic devices from directly dialing 911. Networking across state lines would be much more difficult if not using an ESInet, so until ESInets are available in every state and are capable of networking across state lines, it is impractical to provide improved access from call centers. However, use of the ASAP protocol may provide an interim step of non-voice transfer of information from a call center to ECCs.

Regardless of the answering point for the initial contact by a reporting party, the NPSBN can be used to transport information forwarded by the ECC or to initiate direct contact with the reporting party. Direct contact may be a normal cellular call to the reporting party’s phone or may include conferencing by the ECC to allow audio from the reporting party’s location to be monitored by a field responder.

3.2.6 Intelligent Buildings

Owners and managers of commercial and industrial buildings strive to reduce energy and operational costs through investment in sophisticated energy management systems. The IOT’s emergence enables placement of greater numbers of sensors in buildings to measure temperature, light, and occupancy, and to monitor alarms. Management of vast numbers of sensors will require more complex monitoring systems that are projected to use machine learning and artificial intelligence (AI) to automate functions and to distill complex data into an actionable form.

Alarm data collected by intelligent building systems—such as smoke, fire, and carbon monoxide detectors—may be transmitted to an alarm-monitoring center for verification and forwarding to an ECC. With increased numbers of sensors inside buildings, the accuracy of data that indicates conditions inside the structure will improve. For example, an ability to detect movement in buildings will help emergency responders pinpoint areas that should be searched and evacuated first; further, sensors will alert of the presence of smoke or fire in stairways or corridors, as well as the location of activated sprinklers. Firefighters will have access to this information and be able to pull down building plans through the NPSBN to compare information, allowing them to pinpoint the source as well as understand the building they are walking into, as well as the need for any special equipment based on their analysis of this combined information.

Routing of alarms through use of ASAP via NLETS or through a new IP network interface connection may be practical alternatives for receipt of IoT-originated notifications. Based on National Information Exchange Model (NIEM) 2.0 should be able to be leveraged to create a variety of new interfaces, not only for alarms but for any type of call where the data fields are consistent. In any event, some method of screening alarm calls or signals from devices to reduce false alarms will be required.

3.2.7 IoT Devices

The IoT marketplace is emerging rapidly and exponentially. IHS Markit, a technology market consultant, estimates[7] the current number of IoT devices to be 35 billion. Generally, IoT devices are simple and intended to communicate information at a slow data rate to a central location and, in some cases, to control other devices remotely. Applications are increasing, with early adopter devices focused on areas such as electronics equipment monitoring, system function monitoring and control, alarm and fault reporting, and location tracking. Further, given the vast number of devices that already exist, AI applications are being deployed to help analyze trends and, in some cases, to recommend actions based on this information.

IoT devices are an essential element of smart cities programs. Many applications have been proposed or deployed to measure traffic flow, monitor traffic-control devices, report road surface temperature, measure air-pollution levels and perform other data-collection functions. In conjunction with AI applications, such devices can provide actionable data that, in some cases, may require emergency response.

Some public safety IoT applications will be supported by FirstNet's NSPBN. Others will rely on commercial 4G, 5G and narrowband technologies with connection to the public internet or dedicated secure IP network connections.

Examples of IoT devices that could provide useful information to ECCs include:

- Environmental sensors
  - Radiation sensors in the vicinity of nuclear power plants or facilities

[7] Applying AI & ML to IoT-generated Data; IHS Markit Technology Market Insights, May 23, 2019

  - Air quality – air pollution, ozone, contaminants
  - Chemical or biological hazards
- Traffic-management sensors
  - Congestion
  - Accidents
  - Assistance in routing emergency vehicles based on real-time traffic-flow data
  - Road temperature sensors, e.g., advance warning of icing conditions
  - Traffic-signal control
- Vehicle-tracking devices
  - Public safety vehicles
  - Municipal government vehicles, e.g., snowplows, refuse collection, school buses
  - Vehicle-tracking devices in support of investigations and chases
- Gunshot-detection systems

Information from a vast number of sources requires filtering and analysis in real time, to ensure that it is actionable, without distracting and overloading ECC personnel. An initial planning task concerns the inventory of data sources available from existing governmental systems, such as traffic control, building-monitoring systems, alarm systems, public utility systems, and others. This data needs to be analyzed regarding its applicability to the emergency response system. Data should be evaluated not only on the basis of its potential for reporting an emergency but also for its potential to enhance situational awareness regarding conditions that might improve the effectiveness, timeliness, and safety of emergency responders.

Data sources external to the public safety agency or associated governmental entity (e.g., state, city, county, town) also should be considered and measured to determine their importance or benefit to the emergency response system. Examples are databases maintained by non-governmental organizations, such as medical facilities or services, emergency-response clearinghouses, commercial traffic-information services, broadcast media weather information, and utility companies.

3.2.8 Smart City Sensors

The Smart City Council defines a smart city as one that "... uses information and communications technology (ICT) to enhance its livability, workability, and sustainability. First, a smart city collects information about itself through sensors, other devices, and existing systems. Next, it communicates that data using wired or wireless networks. Third, it analyzes that data to understand what's happening now and what's likely to happen next." Data sources may be from municipal or state sensors or systems operated by private enterprises.

In the ECC environment, information received may be exclusive to public safety, such as that generated by gunshot recognition-and-detection systems. Other information may be of a public nature, such as weather data, e.g., wind speed and direction, precipitation, temperature, humidity, and barometric pressure. This information may be distributed as received or may be processed using AI for predictive purposes.

As a simple example, winter precipitation accompanied by a falling temperature may be predictive of icing conditions that may be accompanied by an increase in vehicular and pedestrian accidents. Such information would be of value to EMS, fire/rescue, and law enforcement personnel, who then would be alerted to drive with increased caution when dispatched to an incident or would anticipate accidents on overpasses and bridges.

Other smart city applications widely reported include traffic-monitoring and asset-management systems. Sensors that measure the volume and speed of traffic can feed applications that manage traffic signals and improve traffic flow. These applications can contribute information to routing applications that will assist emergency responders in choosing the least-congested route to an emergency scene.

Asset management applications using sensors can track the location of municipal vehicles and equipment including public transportation, public works, and utility equipment, Asset-tracking applications can be helpful in locating equipment or personnel needed for an emergency response.

Planning at an early design stage is needed for public safety access to, and inclusion in, such applications. Wireless access to the applications through the NPSBN is practical and will add utility to existing routing and emergency planning applications.

3.2.9 Social Media Inputs

Through the use of the NPSBN, artificial intelligence (AI) software can be leveraged to identify actionable information posted on social media, which will provide actionable data regarding the location and/or nature of the emergency, which then can be forwarded to field responders. Social media monitoring by ECCs and emergency management agencies (EMAs) is becoming more common, especially during emergency or disaster response. In an emergency, the public may turn to social media as an alternative to the 911 system. ECCs may need to consider employing a communications specialist, multimedia analyst or similar position that can monitor and respond to social media reports or inquiries. This position will require internet access, which often is restricted within ECCs. In addition, ECCs will have to become more proactive when dealing with the general public.

3.2.10 Telematics

The NPSBN will enable field responders to access telematics data before and during response. For example, if there is an accident in a rural, mountainous area, understanding the car speed at impact, the type of car, the terrain and how many times the car rolled, will allow EMS to anticipate the type of trauma suffered by passengers and factor that analysis into the decision to send a helicopter or an ambulance, alert the best hospital to handle the anticipated trauma, and provide the resources that likely will be needed during transport. Current production vehicles commonly are equipped with location-determining technology and wireless communications functionality. This functionality is used for reporting emergencies to services such as General Motors' OnStar service. Such services conference emergency calls to ECCs via a ten-digit number, rather than 911; the ability to speak with a crash victim in the immediate aftermath can be vitally important in medical emergencies. Depending on the vehicle type, they also may receive information regarding breakdowns, collisions or rollovers, or airbag deployment as part of automatic crash response or provide information that can be used to track the location of stolen vehicles.

Newer services are being deployed that use the vehicle occupant’s mobile device to detect a crash, by leveraging a special crash-detection algorithm and two-way communications through an app installed on the device.

3.3 Planning for Multimedia Data Interfaces

Future public safety communications systems will be IP-based and as such will enable data sharing between agencies that will enhance emergency response and keep field responders safer. However, data sharing will require an MOU between public safety agencies, particularly ECCs. Examples of such data include the following:

- Multimedia data from persons reporting emergencies
    - Videos or digital images of the scene
- Multimedia data from video surveillance and/or traffic camera networks
- Schools’ panic alarm and video systems

However useful, multimedia content presents yet another challenge for historically understaffed ECCs and their telecommunicators, particularly those who multitask between the call-taking and radio dispatch functions. There is an additional concern that the reception of multimedia data from external sources (911 callers) and internal sources (field responders) could be too distracting or too traumatic for ECC personnel. There are multiple ways this can be managed with many early adopter agencies leading the way.

Multimedia monitoring or analysis units staffed by trained multimedia analysts quickly will become a best practice to provide the live review of inbound video and audio content, sensor alerts and social media content, and then to act on the information received. Units that already are formed—including those that are leveraging an existing SAC, or fusion or intelligence center—are equipped with CAD system interfaces and radio channel access to enable call following and to provide context and updates on the data received.

In addition to CAD and radio system access, to effectively monitor real-time events, the units generally will require mapping interfaces, messaging applications, and a voice-recording system. Video display walls will be required that allow monitoring of fixed camera networks, mobile cameras, and multimedia data associated with dispatch records. Video analytics also may assist in the review of content received from callers, field personnel, and fixed or mobile cameras.

Use of staff trained and armed with the right tools, and skilled in public safety communications operations and practices may provide the optimal solution for reviewing multimedia data. However, this only will be possible if staff are properly trained and provided with the right multimedia analysis tools to do the work.

Configuration and staffing on how to best manage these new roles will vary from locality to locality. Some believe that reception by an ECC of multimedia content may be a distraction to call-takers and dispatchers during busy hours. Others welcome the opportunity for the telecommunicator role to expand into new career opportunities and new ways to help callers and field responders. Some larger ECCs may have staff that have the skill sets to do this, while others may need statewide or regionwide support with training in law enforcement.

In places where a multimedia analysis unit is established on a local, regional, or statewide basis, the ability to receive and distribute inbound multimedia data from and to the NG911 system will be needed. If managed internally the associated data can be routed and cooperatively handled by the call-taker and the multimedia unit. If the unit is staffed externally and on a 24-hour basis, the most desirable capability would be to receive data at the same time as the associated ECC. In this scenario, a less-desirable option is to receive multimedia data that has been forwarded by an ECC. If routing of multimedia data from an ECC is automated, the possibility of delay resulting from human intervention will be reduced. Inbound data from emergency responder personnel or vehicles should be routed automatically to the external unit and ECC.

It is essential to the efficiency of future call processing that technologies such as AI and machine-to-machine learning be deployed to analyze the intense volume of data that will become available, so that what is presented to a telecommunicator is accurate, timely and actionable rather than a lot of noise and distraction.

3.3.1 Multimedia Servers

Reception, viewing, routing, archiving, and retrieving multimedia data will require implementation of networked servers and data-analytics applications. Multimedia servers may be hosted in the cloud by a service provider, may be operated on a state or regional basis, or may be located at the ECC or its associated data center. Multimedia servers will need to be connected to an IP network to provide interfaces to the CAD system, to FirstNet’s NPSBN, to other broadband wireless networks, to a public safety enterprise network, or to an RMS for EMS, fire/rescue or law enforcement.

Archival of all multimedia data received in the ECC, regardless of source, will be required. Such archival will be needed for both raw data as well as edited data. For example, a caller reporting an incident may transmit a video file several minutes in duration (raw data). A clip of this video, which contains salient information, may be distributed to field responders (edited data). Investigators may, in the future, need to review the entire raw video data file for additional details or to establish the context of the information it contains. Provision of video files under a subpoena likely will require all raw data files related to an incident.

It can be assumed that multimedia data will be used as evidence in investigation and prosecution of crimes. Alternatively, multimedia data may be considered medical records, which are protected by the Health Insurance Portability and Accountability Act (HIPAA). Document-retention requirements for these two circumstances are neither identical nor consistent. A legal analysis of document-retention requirements is outside the scope of this report. New state-level guidelines may be required for the preservation and release of multimedia data received by an ECC.

Because multimedia data may be used as evidence in judicial proceedings, an audit trail must be provided in the multimedia data-management system. An audit trail should provide, at a minimum, the time and date received, origin, destination of routed content, file size, file type, date and time opened and viewed, identity of person opening the file, edited files derived from raw data, record number, and CAD record or incident number.

An MOU or another policy document that governs privacy, retention, and access to multimedia data may be required in cases where an ECC, SAC, or other entity serves multiple public safety agencies. Such a document would reflect the differences in requirements between EMS, fire/rescue and law enforcement data.

In addition to local area network (LAN) access to the multimedia data-management system, data will be routed outbound from, and inbound to, the system. Routing likely will be required within the ECC's ecosystem of users as well as with outside agencies and facilities.

Whether managed in-house, through a partnership or outsourced altogether, ECCs will need to have the ability to include the results of this actionable data to improve situational awareness, response times and ultimately emergency response outcomes.

3.3.2 Inbound Routing of Multimedia Data

Inbound routing of multimedia data refers to the reception of data that originates outside of the ECC from emergency responders, autonomous devices, or the public. This data is discussed by source in the following subsections.

3.3.2.1 Video Sent from Public Safety Vehicles

Vehicle-mounted camera systems are commonplace in law enforcement vehicles but generally, are used for archival purposes. The presence of a mobile router on a wireless broadband network, such as FirstNet's NPSBN, will enable video and audio streaming from a suitably equipped vehicular camera system to the ECC and/or to a multimedia analysis unit, surveillance center or SAC. Vehicle-mounted cameras may include dash cameras, proximity cameras—side or rear facing—or interior cameras in the vehicle's prisoner-retention area.

As is the case with body-worn cameras, vehicle-mounted cameras could provide additional safety for field responders by enabling trained personnel to observe the situation without distraction. Fire service video might include dash-camera video, cameras mounted on aerial apparatus, or firefighter body-worn cameras. This information may be of importance to a SAC that is focused on fireground operations and/or firefighter accountability and safety. This multimedia data may be stored onsite, or by a cloud service.

Application of vehicle-mounted cameras in fire apparatus is focused frequently on dash-mounted cameras that record events in front of the apparatus. Steerable cameras combined with a broadband vehicular router could be applied to provide streaming video of a fire or accident scene to the ECC or a fire command center.

3.3.2.2 Video Sent by Emergency Responders Outside of Vehicles

Provision and sharing of accurate location data may improve the safety of emergency responders by supporting better tactical decision support, adding the ability to track personnel outside of a vehicular environment, and supporting mapping of resources for planning and deployment decisions. Components of effective use of location data include:

- GIS with detailed premises mapping
- Access to third-party mapping information, satellite imagery, and photogrammetry
- Implementation of automatic vehicle location (AVL) and access to mapping both in the ECC and in the field
- Equipping field responders with wireless devices that provide personal location and tracking in real time when they are outdoors, and ultimately when indoors
- Geofencing to focus tracking within a perimeter, search area, an evacuation area, or another geographic area of interest

3.3.2.2 Video from a Caller

Video from the caller side will be an important component of telemedicine. Parties reporting medical emergencies may choose to send video to the ECC that provides information on the medical condition of a patient or the circumstances of an injury or illness. Due to the resource intensive nature of receiving video from callers, this information may be stored and forwarded to the responding units via the NPSBN.

Patient-side video and biometric data may be transmitted from an ambulance or EMT body-worn device to a medical professional at a hospital or other facility. This information likely is to be used for medical consultations that may assist in the trend to reduce repeat trips to hospital emergency departments where no hospital admissions occur. This information likely will be a portion of the patient record and will be protected by HIPAA. Generally, such patient-side video would not be sent to an ECC or SAC for storage.

Receiving video from callers will need to be coordinated carefully. It may be possible to address video only during normal or predictable call-volume loads. If a major event occurs, ECC staff and field responders may not have the resources to review each video sent or video chat with every person. This surge in capacity will need to be managed and road mapped by working out agreements with other ECCs to handle the overload or by utilizing EOCs and video analytics. Specialized training may be required to utilize video effectively.

3.3.2.3 Video from Other ECCs

- There are several situations in which planning is required for inter-ECC transmission of multimedia data. 911 calls routed incorrectly to an ECC may be transferred to another ECC and multimedia data sent by the reporting party should accompany the transferred call.

- Multimedia data regarding a missing person, a suspect, or a wanted vehicle will need to be shared between ECCs or sent directly via the NPSBN to field units in accordance with a “be on the lookout” (BOLO) plan.

- Maps and other images may be shared between ECCs for situations such as street closings, parade routes, and other events.

Multimedia data sharing may be accomplished via an ESInet, a separate wide-area network (WAN), or in some situations, by wireless connection to the NPSBN. Regionalization of multimedia data storage may be desirable for cost sharing and compatibility of platforms in use.

3.3.2.4 AI Content Analytics

Video analytics have the potential to enhance the safety of firefighters and enable an informed decision regarding how the fire will be attacked. Access to video generated by apparatus-mounted or fixed cameras will be facilitated by the NPSBN. Such video, once it is assessed using analytics software, then may be shared with responding units, chiefs, and intelligence centers, also via the NPSBN. Firefighters will find value in the use of video analytics in terms of smoke analysis. Thick, billowing smoke is indicative of hydrocarbon combustion, which elicits hydrogen cyanide. Grey, puffing smoke with brown tinges represents un-combusted material looking for the right combination of oxygen, fuel, and heat before it explodes in a backdraft.

Video analytics combine AI with video playback. AI platforms use known images to “train” the software to recognize similar objects while rapidly scanning video recordings. Images may include facial recognition, vehicles, animals, profiles/positions of persons (e.g., person down, threatening behavior) and weapons. Introduction of AI into video analytics will enable review of lengthy recordings, such as from video surveillance and security cameras. Video analytics can be applied to videos sent by 911 callers, particularly raw video that is lengthy. Video analytics can be applied to the review of large video files such as archived dash- or body-camera data. Unless deployed very near to the data source, video analytics applications are less likely to be useful as a tool in the ECC compared with an investigative capacity.

Application of voice analytics to multimedia data collected from 911 reporting parties and emergency responders should be facilitated by the multimedia data system. For law enforcement applications, an ability to parse the voice content of a video clip and apply analytic routines to provide voiceprints or patterns of words or speech will be desirable as a future application.

An ability to recover text information from images or copies of documents sent to the ECC will be a useful function. Analytics provided by other applications—such as handwriting recognition, type fonts, word usage, and patterns—should be supported by the multimedia data system.

3.3.3 Outbound Routing of Multimedia Data

Wireless data-equipped personnel will require a connection between the multimedia data-management system and the broadband wireless network(s) in use by the agencies served by the ECC. This connection will need to be dimensioned to handle large multimedia files with minimal latency. A connection with quality-of-service (QoS) guarantees is desirable, such as the Accelerated Virtual Private Network (AVPN). The connection needs to be firewall-protected and servers must be equipped with virus and malware protection.

3.3.3.1 Cybersecurity Measures

Malware and unwanted executable programs can disrupt critical networks unless adequately protected by cybersecurity measures. Introduction of the NPSBN or other wireless networks into the public safety enterprise creates new opportunities for hackers to attempt to penetrate the protections currently in place.

New sources of threats include the use of privately owned wireless devices, pad computers and other home computers that are not protected at the same level as enterprise computers. Such devices can propagate malware behind the firewall of an enterprise network.

Cybersecurity software and service providers recommend a multitiered approach to cybersecurity. Endpoints on a network are user computers, terminals, and devices. Such devices have as their first line of defense antivirus and antimalware software. Most are password protected and have a firewall function. Dual authentication of users is employed increasingly. Endpoints can be exploited by malware and can propagate that malware to servers and other users on a network. It is important that endpoints employ the enterprise cybersecurity protection, which argues against the use of personal devices on a public safety enterprise network. Current cybersecurity technology employs techniques such as behavior-based analytics that search for known and unknown threats on groups of endpoints. Searches can reveal whether an attack occurred and whether it was spread to other endpoints or network devices.

- Network Security – Most networks employ firewalls and secure web gateways to protect against attacks. Sophisticated hackers employ polymorphic techniques to exploit vulnerabilities in operating systems and applications to introduce malware. Webroot defines polymorphism as “…a tactic designed to circumvent traditional antimalware solutions, which use names, encryption keys, signatures, or hashes to detect a single instance of malware delivered to a large number of people.”[8] Polymorphic attacks now use sophisticated algorithms to randomize the numeric keys to avoid detection by antivirus or antimalware applications.

  In addition to basic approaches to network security, additional steps should be taken to protect against malware introduced from internet connections to the public safety enterprise network. Such steps include appliances that monitor lateral and outbound traffic on the network, and through machine learning, can identify suspicious activity on the network.

  An additional step for network administrators is to consider contracting with a service provider that offers alerts of trending malware attacks from domestic and international sources. Such service often is

[8] 2018 Webroot Threat Report

provided by suppliers of security appliances. Cloud-based network monitoring is a trending service for agencies with limited internal capabilities.

Mobile Device Security – Mobile devices are an additional source of threats from malware. Use of personal devices for public safety functions increases the risk of introduction of malware installed from the internet. Uniform security policy and installation of management and anti-malware tools on all wireless devices connected to public safety enterprise networks is the best practice for malware prevention.

Introduction of wireless devices to public safety enterprise networks requires both policy development and software systems to provide the needed security. Multiple steps are required to implement a secure mobile environment. Responsibility for the administration of mobile devices needs to be established by an enforceable policy. Both wireless devices and applications need to be covered by an "onboarding" policy and procedure wherein the devices are configured to comply with cybersecurity rules.

A designated administrator will be needed to manage what is referred to by FirstNet as "local control." This function manages onboarding, i.e., additions, changes and deletions of mobile devices on FirstNet's NPSBN. Interoperability permissions needed for access to PTT talkgroups on the NPSBN—as well as Inter-RF Subsystem Interface (ISSI) or other interconnections to LMR systems—are managed through the local control portal, which provides a view of all mobile devices associated with an AT&T account on the NPSBN. Other local control functions include vetting of users and establishment of priority.

Mobile application onboarding may be a new experience for IT administrators. Many applications are available for wireless devices. Such applications may spread malware that can infiltrate public safety information systems. Vetting of applications is required before they are considered for installation on public safety wireless devices. Generally, no application should be installed unless it has been vetted by the FirstNet lab or by the Google Play or Apple stores. Applications should be "whitelisted" by the agency's IT administrator.

CJIS compliance – Mobile devices must comply with Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, 06/01/2019, CJISD-ITS-DOC-08140-5.8, Federal Bureau of Investigation (FBI) Criminal Justice Information Services Division. This reference is available at https://www.fbi.gov/file-repository/cjis-security-policy_v5-8_20190601.pdf/view. The applicable section of this document is Policy Area 13 – Mobile Devices, which governs wireless devices such as smartphones, Wi-Fi access points, air cards, and mobile routers. To implement the requirements of the CJIS policy, a mobile device management (MDM) system is needed to perform security functions.

An MDM is contemplated to provide centralized administration of all public safety wireless devices connected to the enterprise public safety network. At a minimum the MDM must be configured and implemented to exercise the following controls:

- Remote locking of wireless devices

- Remote wiping of wireless devices
- Setting and locking device configuration
- Detection of devices that have been “rooted” (administrative privileges) or “jailbroken” (like rooting, on Apple iPhones, etc.)
- Enforcement of folder or disk-level encryption
- Application of mandatory policy settings on the device
- Detection of unauthorized configurations
- Detection of unauthorized software or applications
- Ability to determine the location of agency-controlled devices
- Prevention of unpatched devices from accessing CJIS and related systems
- Automatic device wiping after a specified number of failed access attempts

Use of an MDM allows the IT administrator to push updates and patches to mobile devices to maintain the security of the public safety enterprise network.

Challenges to conformance with the CJIS cybersecurity policy are generated by “bring your own device” (BYOD) smartphones used by public safety personnel. Access to CJIS data by devices not owned by the public safety entity cannot be provided unless users of such devices consent to the restrictions imposed by the MDM. Access to location data on BYOD smartphones is required, and compliance concerning the whitelisting of applications is difficult to enforce unless the device has been configured under the MDM system.

Access to non-CJIS legacy applications, such as computer-aided dispatch and mapping generally will require the development of mobile applications and interfaces. Several of the major CAD suppliers have such interfaces and applications available for certain versions of their software.

It should be noted that AT&T-FirstNet operates a dedicated security operations center (SOC) to protect its network from cyberattacks. This is a continuously staffed function within AT&T that monitors cyberactivity worldwide. Its intent is to identify and quickly remediate certain kinds of cybersecurity threats, such as DDOS attacks, that can cripple data networks.

3.3.3.2 Other ECCs

Data sharing between ECCs is a desirable function. Sharing of multimedia data regarding people, vehicles, and incidents should be supported by the ESInet or by a secure WAN connection. Regionalization of multimedia data networks may be a more efficient method of provisioning this service.

3.3.3.3 Other Public Safety Agencies

Interoperability with public safety agencies other than ECCs that supports multimedia data sharing should be supported. This interoperability may be provided by connection to a WAN or via a mobile device connection enabled by FirstNet’s NPSBN or another broadband wireless network.

3.3.3.4 Public Alerts

It may be desirable to share with the general public some screened multimedia data such as images of missing children (Amber Alerts), missing senior citizens (Silver Alerts), or persons/vehicles wanted in connection with criminal activity. By necessity, this connection would be via the internet. It is recommended that this connection not be made with the internal LAN at an ECC or SAC; rather, the data should be transferred offline to a public-facing network connection.

3.3.4 Between Call-Takers and Radio Dispatchers

Still images or short video clips that are received by 911 call-takers from a person reporting an emergency should be attached to an incident dispatch record when transferred to a radio dispatcher. This information also should be accessible from a field responder equipped with a mobile computer or smartphone. Generally, this can be accomplished by an interface to the CAD system via FirstNet's NPSBN.

3.4 Recommended Areas of Future Focus

Implementation of the transformational technology will require development of guidelines and practices that will be needed to quantify the financial, operational, and technology needs of the ECCs. The Program has an important role in working with the ECC partners to assist in developing the guidelines and practices that will be applicable to all ECCs in Michigan. Those involved in the planning will need to consider the following:

- How will ECCs and field responders manage all of the enhanced data functions during high-traffic events?
- How will ECCs integrate with FirstNet regarding technology, operational and non-traditional cost impacts?
- How will ECCs analyze large amounts of data coming in from the public for relevance?
- How can technologies, such as video analytics, be leveraged to prioritize video traffic?
- What legal, retention, and data-storage issues present themselves from this convergence?

Additionally, joint NG911/NPSBN state-level planning is essential for success. This will aid in the implementation of change-management programs at the local, regional and state levels to evaluate considerations for determining implementation of proposed next-generation solutions that leverage FirstNet's NPSBN to improve emergency response through improved situational awareness, decreased response times and enhanced potential to save lives. These include technology, workforce, operational, policy/governance, regulatory, and funding issues that limit or prevent interoperability between NG911 systems and the NPSBN. To further support this convergence, agencies should identify areas where systems and resources can be shared between NG911 systems and the NPSBN. Lastly, this only can be successful if educational programs that support executive, support, operations, and IT staff are established.

4 Conclusion

Multimedia data streams made possible by the NPSBN and NG911 systems have the potential to provide ECCs with unprecedented situational-awareness information that will make both telecommunicators and field responders more effective, resulting in enhanced emergency response, more lives and property saved, and safer responders. To fully leverage this capability, ECC managers will be confronted with technical, financial, operational and personnel development challenges. As with implementation of other transformational technologies, there will be cultural and procedural changes that will need to be anticipated and managed.

ECC personnel interviewed by Mission Critical Partners (MCP) on behalf of the Michigan Public Safety Broadband Program have the basic systems and procedures in place to handle 911 calls and to provide connectivity to emergency responders via wireless data networks. Michigan is considered an early adopter in terms of NG911 technology and deployment of a statewide ESInet. However, gaps exist in the reception, distribution and archiving of multimedia data that will be available when the NPSBN and NG911 systems are deployed and fully operational. Planning is required to define and quantify a variety of technical impacts, from interfacing with myriad data sources to managing, storing and securing the data.

Success measurement will be determined by achievement of the project goals and objectives. After deciding to implement any of the previously described interfaces, ECC managers should ensure that the project addresses the items described in Section 2.1 above.

The most important question with any implementation is this: does the proposed solution improve emergency response outcomes? If the answer is yes, then the project, if implemented correctly, can be successful. Once that is established, the next step in this process is to develop a detailed planning document to establish a path to adopting FirstNet's NPSBN and integrating it with NG911.

Prepared by

MissionCriticalPartners
Because the Mission Matters

State College Office | 690 Gray's Woods Blvd. | Port Matilda, PA 16870 | 888.8.MCP.911 or888.862.7911

This project is supported by SLIGP 2.0, awarded by the National Telecommunications and Information Administration (NTIA), National Institute of Standards and Technology (NIST), U.S. Department of Commerce (COD), and administered by the Michigan State Police (MSP). Points of view or opinions contained within this document do not necessarily represent the official position or policies of the MSP or the DOC.

Michigan's Public Safety Broadband Program